Milnor K-groups attached to elliptic curves over a p-adic field

Toshiro Hiranouchi

September 17, 2012

Abstract

We show the injectivity of the Galois symbol for the Milnor K-group attached to elliptic curves over a p-adic field under some assumptions. As by-products, over the p-adic field we give the structure of the abelian fundamental group of an elliptic curve and the structure of the Chow group for the product of elliptic curves.

1 Introduction

K. Kato and M. Somekawa in [11] introduced the Milnor type K-group $K(k; G_1, \dots, G_q)$ attached to semi-abelian varieties $G_1, \dots, G_q$ over a field k which is now called the Somekawa K-group. The group is defined by the quotient

$$K(k; G_1, \dots, G_q) := \left(\bigoplus_{E/k:\,\text{finite}} G_1(E) \otimes \cdots \otimes G_q(E) \right) / R \tag{1}$$

where R is the subgroup which produces "the projection formula" and "the Weil reciprocity law" as in the Milnor K-theory (Def. 2.2). As a special case, for the multiplicative groups $G_1 = \cdots = G_q = \mathbb{G}_m$, it is nothing other than the ordinary Milnor K-group of the field k as $K(k; \mathbb{G}_m, \dots, \mathbb{G}_m) \xrightarrow{\simeq} K_q^M(k)$ ([11], Thm. 1.4). For any positive integer m prime to the characteristic of k, Somekawa defined also the Galois symbol map

$$h : K(k; G_1, \dots, G_q)/m \to H^q(k, G_1[m] \otimes \cdots \otimes G_q[m])$$

by the similar way as in the classical Galois symbol map $K_q^M(k)/m \to H^q(k, \mu_p^{\otimes q})$ on the Milnor K-group and the map h was conjectured to be injective over arbitrary field k. For the case $G_1 = \cdots = G_q = \mathbb{G}_m$, the conjecture holds by the Milnor-Bloch-Kato conjecture, now is the theorem of Voevodsky, Rost, and Weibel ([15]). However, it is also known that the above conjecture does not hold in general (see remarks Conj. 2.3 below for the other known results).

The aim of this note is to show this conjecture for elliptic curves over a local field under some assumptions.

Theorem 1.1 (Thm. 4.1, 4.3)**.** *Let k be a finite extension of $\mathbb{Q}_p$ for $p \neq 2$. Let X and X' be elliptic curves over k with $X[p^n] \subset X(k)$ and $X'[p^n] \subset X'(k)$.*

(i) *The conjecture holds for $G_1 = \mathbb{G}_m$ and $G_2 = X$ on $m = p^n$.*

(ii) *Assume that X has semi-ordinary reduction, in other words, X is not a supersingular elliptic curve. Then the conjecture holds for $G_1 = X$ and $G_2 = X'$ on $m = p^n$.*

After Raskind-Spieß [8] here we call X has *semi-ordinary* reduction if it has good ordinary or split multiplicative reduction. The assertion (i) in the above theorem is known for arbitrary field due to Spieß so we give a merely alternative and an elementary proof. On the assertion (ii) also, some parts of the theorem have already known. Since we are assuming $p \neq 2$, by taking a finite extension, we may assume that X and X' have at worst split multiplicative reduction. The injectivity of h is known for both of X and X' have semi-ordinary reductions ([16], [8], see also [7]). Hence our main interest is in supersingular elliptic curves.

In our previous paper [3], we studied the image of the Galois symbols for elliptic curves X and X'. Putting the above theorem together, we obtain results on the structure of the Somekawa K-groups as follows. (Precisely, in [3] we did not refer on the image of the Galois symbol for $\mathbb{G}_m$ and X as in the assertion (i). However, the same proof works and easy to show.)

Corollary 1.2. *Let X and X' be as above.*

(i)
$$K(k; \mathbb{G}_m, X)/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } X\text{: split multiplicative,} \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \text{if } X\text{: good reduction.} \end{cases}$$

(ii) *Assume that X has semi-ordinary reduction. Then we have*

$$K(k; X, X')/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \textit{if both } X \textit{ and } X' \textit{ have same reduction type,} \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \textit{otherwise.} \end{cases}$$

As byproducts of the assertion (i) above, one can determine the structure of the abelian étale fundamental group $\pi_1(X)^{\mathrm{ab}}$ of the elliptic curve X over k utilizing the class field theory of curves over local fields (Thm. 5.1). On the other hand, the assertion (ii) gives the structure of the Chow group $\mathrm{CH}_0(X \times X')$ of 0-cycles on $X \times X'$ (Thm. 5.2).

Now we give an outline of this paper. In Section 2, first we recall the definition and some properties of Somekawa K-groups $K(k; G, G')$ attached to semi-abelian varieties G and G' over arbitrary field k. Here, we also introduce the Mackey product $G \overset{M}{\otimes} G'(k)$ of G and G' which is defined as in (1) but by factoring our a relation concerning the "projection formula" only. That is why we have the canonical surjection

$$G \overset{M}{\otimes} G'(k) \twoheadrightarrow K(k; G, G')$$

in general. In the proof of our theorems, this product $G \overset{M}{\otimes} G'(k)$ plays an important role. In fact, we will show the injectivity of not only the Galois symbol on the Somekawa K-group but also the composition

$$G \overset{M}{\otimes} G'(k)/p^n \twoheadrightarrow K(k; G, G')/p^n \xrightarrow{h} H^2(k; G[p] \otimes G'[p])$$

if G and G' are elliptic curves. In Section 3 we study the structure of the Mackey product $\overline{U}^m \overset{M}{\otimes} \overline{U}^n(k)$ over a p-adic field k. Here, $\overline{U}^m$ is the Mackey functor defined by the higher unit groups of finite extensions over k as a sub Mackey functor of the cokernel $\mathbb{G}_m/p$ of the multiplication by p on $\mathbb{G}_m$. Tate [14], Raskind and Spieß [8] show that the Galois symbol map induces bijections

$$h^2 : \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \simeq K_2(k)/p \overset{h}{\simeq} H^2(k, \mu_p^{\otimes 2}) \simeq \mathbb{Z}/p.$$

We calculate the kernel and the image of the composition

$$h^{m,n} : \overline{U}^m \overset{M}{\otimes} \overline{U}^n \to \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \xrightarrow{h^2} \mathbb{Z}/p$$

and determine the structure of $\overline{U}^m \overset{M}{\otimes} \overline{U}^n$ partially. The proofs of Theorem 1.1 above shall be given in Section 4 by relating the Galois symbol map on elliptic curves and the above map $h^{m,n}$. In Section 5, we will discuss about the applications on the structure of the abelian fundamental group of an elliptic curve and the Chow group of the product of elliptic curves as noted above.

Throughout this note, for an abelian group A and a non-zero integer m, let $A[m]$ be the kernel and A/m the cokernel of the map $m : A \to A$ defined by multiplication by m. For a field F, For a discrete valuation field K, we denote by $G_F := \mathrm{Gal}(\overline{F}/F)$ the absolute Galois group of F and $H^i(F, M) := H^i(G_F, M)$ the Galois cohomology group of G_F for some G_F-module M.

Acknowledgments. A part of this note was written during a stay of the author at the Duisburg-Essen university. He thanks the institute for its hospitality. This work was supported by KAKENHI 21740015.

2 Somekawa K-groups

In [11] (see also [12]), the Milnor K-group $K(k; G_1, ..., G_q)$ attached to semi-abelian varieties $G_1, ..., G_q$ over a field k is defined by a quotient of the product as Mackey functors $G_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} G_q(k)$. Here, a *semi-abelian variety* is an algebraic group which has a canonical decomposition $0 \to T \to G \to A \to 0$ with a torus T and an abelian variety A.

First we recall that the definition of the Mackey functor and its product. Let k be a perfect field. A *Mackey functor* A is a co- and contravariant functor from the category of étale schemes over k to the category of abelian groups such that $A(X_1 \sqcup X_2) = A(X_1) \oplus A(X_2)$ and if

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ Y' \arrow[r, "g"] & Y \end{tikzcd}$$

is a Cartesian diagram, then the induced diagram

$$\begin{tikzcd} A(X') \arrow[r, "{g'}_*"] & A(X) \\ A(Y') \arrow[u, "{f'}^*"] \arrow[r, "g_*"] & A(Y) \arrow[u, "f^*"'] \end{tikzcd}$$

commutes. It is uniquely determined by its value $A(E) := A(\mathrm{Spec}(E))$ on finite field extensions E over k. A typical example is the one given from a G_k-module A which is defined by $E \mapsto A^{G_E} = H^0(E, A)$ for a finite extension field E over k with norm and restriction maps, where $G_k := \mathrm{Gal}(\overline{k}/k)$ is the absolute Galois group of the field k.

Definition 2.1. For Mackey functors $A_1, \dots, A_q$, their *Mackey product* $A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k)$ is defined by the quotient

$$A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k) := \left(\bigoplus_{E/k:\,\mathrm{finite}} A_1(E) \otimes \cdots \otimes A_q(E) \right) /R,$$

where R is the subgroup generated by elements of the following form:
(PF) For any finite field extensions $k \subset E_1 \subset E_2$, and if $x_{i_0} \in A_{i_0}(E_2)$ and $x_i \in A_i(E_1)$ for $i \neq i_0$, then

$$j^*(x_1) \otimes \cdots \otimes x_{i_0} \otimes \cdots \otimes j^*(x_q) - x_1 \otimes \cdots \otimes j_*(x_{i_0}) \otimes \cdots \otimes x_q,$$

where $j : \mathrm{Spec}(E_2) \to \mathrm{Spec}(E_1)$ is the canonical map.

This gives a tensor product in the abelian category of the Mackey functors with unit $\mathbb{Z} : E \mapsto \mathbb{Z}$ which is the Mackey functor given by identity maps on $\mathbb{Z}$. In particular, for any field extension k'/k and the canonical map $j = j_{k'/k} : k \hookrightarrow k'$, the pull-back

$$\mathrm{Res}_{k'/k} := j^* : A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k) \longrightarrow A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k')$$

is called the *restriction map*. If the extension k'/k is finite, then the push-forward

$$N_{k'/k} := j_* : A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k') \longrightarrow A_1 \overset{M}{\otimes} \cdots \overset{M}{\otimes} A_q(k)$$

is given by $N_{k'/k}(\{x_1, \ldots, x_q\}_{E'/k'}) = \{x_1, \ldots, x_q\}_{E'/k}$ on symbols and is called the *norm map*. Here we wrote $\{x_1, \ldots, x_q\}_{E/k}$ for the image of $x_1 \otimes \cdots \otimes x_q \in A_1(E) \otimes \cdots \otimes A_q(E)$ in the product. Note also that the product $- \overset{M}{\otimes} A$ is right exact for any Mackey functor A.

An algebraic group G over k forms a Mackey functor. For a field extension E_2/E_1, the pull-back is the canonical map given by $j : E_1 \hookrightarrow E_2$ which is denoted by $j^* = \mathrm{Res}_{E_2/E_1} : G(E_1) \hookrightarrow G(E_2)$. For simplicity, we identify the elements in $G(E_1)$ with its image in $G(E_2)$ and the restriction map Res_{E_2/E_1} will be sometimes omitted. If the extension E_2/E_1 is finite, the push-forward is written as $j_* = N_{E_2/E_1} : G(E_2) \to G(E_1)$ and is refereed as the norm map.

Next we recall the definition of the Somekawa K-group $K(k; G_1, \ldots, G_q)$ attached to semi-abelian varieties $G_1, \ldots, G_q$ over k. In this paper, we consider the special case $q = 2$ over the perfect field k. Therefore, consider two semi-abelian varieties G and G' over k.

Definition 2.2. The Milnor K-group attached to G and G' which is called the *Somekawa K-group* is defined by

$$K(k; G, G') := \left(G \overset{M}{\otimes} G'(k) \right) / R,$$

where R is the subgroup generated by the elements of the following form:
(WR) Let $k(C)$ be the function field of a projective smooth curve C over k, $h \in k(C)^\times, f \in G(k(C))$ and $f' \in G'(k(C))$. For each closed point P of C, let $k(C)_P$ be the fraction field of the completion $\widehat{\mathcal{O}}_{C,P}$ of $\mathcal{O}_{C,P}$ by the normalized valuation v_P and $k(P)$ the residue field of $k(C)_P$. For the set of closed points C_0 in C, put $S := \{P \in C_0 |\ f \in G(\widehat{\mathcal{O}}_{C,P})\}$. Assume that $f' \in G'(\widehat{\mathcal{O}}_{C,P})$ for each $P \notin S$. Then,

$$\sum_{P \notin S} \partial_P(h, f) \otimes f'(P) + \sum_{P \in S} f(P) \otimes \partial_P(h, f') \in R.$$

Here $f(P)$ is the image of f by the canonical map $G(\widehat{\mathcal{O}}_{C,P}) \to G(k(P))$ and $\partial_P : k(C)^\times \times G(k(C)) \to G(k(P))$ is the local symbol (for the precise definition, see [11], [12]).

We also denote by $\{x, x'\}_{E/k}$ the image of $\{x, x'\}_{E/k} \in G \overset{M}{\otimes} G'(k)$ in $K(k; G, G')$ for some finite extension E/k. For any extension k'/k, set

$K(k'; G, G') := K(k'; G \otimes_k k', G' \otimes_k k')$. The restriction map on the Mackey product induces a canonical homomorphism

$$\mathrm{Res}_{k'/k} : K(k; G, G') \longrightarrow K(k'; G, G').$$

If the extension k'/k is finite, the norm map on Mackey functors induces

$$N_{k'/k} : K(k'; G, G') \to K(k; G, G').$$

For any isogeny $\phi : G \to H$ of semi-abelian varieties, the exact sequence $0 \to G[\phi] \to G \xrightarrow{\phi} H \to 0$ gives the injection

$$h^1_\phi : H(k)/\phi G(k) \to H^1(k, G[\phi]).$$

Denote by H/ϕ the Mackey functor defined by the cokernel of ϕ. The correspondence is given from $E \mapsto H(E)/\phi G(E)$. For two isogenies $\phi : G \to H$ and $\phi' : G' \to H'$, the cup product and the norm map (=the corestriction) on the Galois cohomology groups give a map $\widetilde{h}^2$ as follows:

$$\begin{tikzcd} \bigoplus_{E/k} H(E) \otimes H'(E) \arrow[r, "h^1_\phi \otimes h^1_{\phi'}"] \arrow[d, "\widetilde{h}^2"] & \bigoplus_{E/k} H^1(E, G[\phi]) \otimes H^1(E, G'[\phi']) \arrow[d, "\cup"] \\ H^2(k, G[\phi] \otimes G'[\phi']) & \bigoplus_{E/k} H^2(E, G[\phi] \otimes G'[\phi']) \arrow[l, "N_{E/k}"'] \end{tikzcd} \tag{2}$$

where E runs through all finite field extension of k and $\cup$ is the cup product of the Galois cohomology groups. The map $\widetilde{h}^2$ factors through the product of the Mackey functors $H/\phi \overset{M}{\otimes} H'/\phi'(k)$ (*cf.* [11], Prop. 1.5) and we obtain

$$h^2_{\phi,\phi'} : H/\phi \overset{M}{\otimes} H'/\phi'(k) \to H^2(k, G[\phi] \otimes G'[\phi']) \tag{3}$$

which is called *the Galois symbol*.

For any positive integer m prime to the characteristic of k, as a special case, we consider the isogenies $m : G \to G$ and $m : G' \to G'$ induced from the multiplication by m. The Galois symbol $h^2_{m,m} : G/m \overset{M}{\otimes} G'/m \to H^2(k, G[m] \otimes G'[m])$ defined above (3) factors through $K(k; G, G')/m$ ([11], Prop. 1.5) and the induced homomorphism

$$h^2_m : K(k; G, G')/m \to H^2(k, G[m] \otimes G'[m])$$

is also called the *Galois symbol*. On the Galois symbol map, Kato and Somekawa presented the following conjecture.

Conjecture 2.3 (Kato-Somekawa, [11]). *Let G and G' be semi-abelian varieties over arbitrary field k. For any positive integer m prime to the characteristic of k, the Galois symbol h^2_m is injective.*

It is easy to see that the surjectivity of the Galois symbol does not hold in general. (As examples we will refer some precise calculations of the image in some special cases below, see (4).) The above conjecture is studied in the following special semi-abelian varieties:

(a) *The case of $G = G' = \mathbb{G}_m$*: The conjecture and more strongly the bijection of the Galois symbol are known for the multiplicative groups $\mathbb{G}_m = G = G'$ by the Merkurjev-Suslin theorem [6]. In fact, the K-group $K(k; \mathbb{G}_m, \mathbb{G}_m)$ coincides with the Milnor K-group $K_2^M(k)$ ([11], Thm. 1.4) and the map h^2 is the ordinary Galois symbol.

(b) *The case G and G' are tori*: Yamazaki proved this conjecture for tori which admit *motivic interpretations* ([17], Prop. 2.11) and disproved it for general tori with M. Spieß ([12], Prop. 7). Hence the above conjecture does not hold in general.

(c) *The case $G = \mathbb{G}_m$ and G' is a Jacobian variety*: It is known also (by Spieß, [16], Appendix) the conjecture holds over an arbitrary field k for $G = \mathbb{G}_m$ and $G' = J_X$ the Jacobian variety of a smooth projective geometrically connected curve X over k.

We have the following observations.

Lemma 2.4. *Let T and T' be split torus over a field k with characteristic l and A, A' abelian varieties over k. Put $G = T \times A$ and $G' = T' \times A'$.*

(i) *For any primes p and q prime to l, if the Galois symbols h^2_p and h^2_q is injective for G and G', then so is h^2_{pq}.*

(ii) *For a prime $p \neq l$, assume $G[p^n]$ and $G'[p^n]$ are k-rational. If the Galois symbols h^2_p and $h^2_{p^{n-1}}$ is injective for G and G', so is $h^2_{p^n}$.*

Proof. The assertion (i) is easy to show. To show (ii), consider the following diagram with exact rows:

$$\begin{tikzcd}
K(k; G, G')/p^{n-1} \arrow[r] \arrow[d, "h^2_{p^{n-1}}"'] & K(k; G, G')/p^n \arrow[r] \arrow[d, "h^2_{p^n}"'] & K(k; G, G')/p \arrow[d, "h^2_p"'] \\
H^2(k, G[p^{n-1}] \otimes G'[p^{n-1}]) \arrow[r] & H^2(k, G[p^n] \otimes G'[p^{n-1}]) \arrow[r] & H^2(k, G[p] \otimes G'[p]).
\end{tikzcd}$$

The assumptions $G[p^n] \subset G(k)$ and $G'[p^n] \subset G'(k)$ imply the injectivity of the map $H^2(k, G[p^{n-1}] \otimes G'[p^{n-1}]) \to H^2(k, G[p^n] \otimes G'[p^n])$. The assertion follows. $\square$

3 Higher unit groups

Let k be a finite field extension of $\mathbb{Q}_p$ assuming $p \neq 2$. We denote by v_k the normalized valuation, $\mathfrak{m}_k$ the maximal ideal of the valuation ring $\mathcal{O}_k$, $\mathcal{O}_k^\times = U_k^0$ the group of units in $\mathcal{O}_k$ and $\mathbb{F} = \mathcal{O}_k/\mathfrak{m}_k$ the (finite) residue field. In this section we study the Mackey product of the Mackey functors $\overline{U}^m$ defined by the higher unit groups. These are the key results in the proof of the main theorems (=Thm. 4.1 and 4.3 in the next section). On the group $k^\times/p$, the higher unit groups $U_k^m := 1 + \mathfrak{m}_k^m$ induce the filtration $(\overline{U}^m)$ given by $\overline{U}_k^m := \mathrm{Im}(U_k^m \to k^\times/p)$. First we recall that the structure of the graded pieces of this filtration.

Lemma 3.1 (*cf.* [4], Lem. 2.1.3; [1])**.** *Put* $e_0 := e_0(k) := v_k(p)/(p-1)$. *Assume that* $\mu_p := \mathbb{G}_m[p] \subset k$.
(a) *If* $0 \leq m < pe_0$, *then*

$$\overline{U}_k^m/\overline{U}_k^{m+1} \simeq \begin{cases} \mathbb{F}, & \text{if } p \nmid m, \\ 1, & \text{if } p \mid m. \end{cases}$$

(b) *If* $m = pe_0$, *then*

$$\overline{U}_k^{pe_0}/\overline{U}_k^{pe_0+1} \simeq \mathbb{Z}/p.$$

(c) *If* $m > pe_0$, *then*

$$\overline{U}_k^m = 1.$$

Let $\mathbb{G}_m/p$ be the Mackey functor over k defined by the cokernel of the multiplication by p on $\mathbb{G}_m$, that is given by the correspondence $E \mapsto E^\times/p$ for any finite extension E/k and the induced maps by the norms and the canonical inclusion of extensions. Next we consider the Mackey functor $\overline{U}^m$ over k defined as a subfunctor of $\mathbb{G}_m/p$ which is given by

$$E \mapsto \overline{U}_E^{me_{E/k}}$$

for any positive integer m, where $\overline{U}_E^n$ is the subgroup of $E^\times/p$ as above and $e_{E/k}$ is the ramification index of the extension E/k. In particular, the structure of the Mackey functor is given by the norm map

$$N_{E_2/E_1} : \overline{U}_{E_2}^{me_{E_2/k}} \to \overline{U}_{E_1}^{me_{E_1/k}}$$

and the natural map

$$\mathrm{Res}_{E_2/E_1} : \overline{U}_{E_1}^{me_{E_1/k}} \to \overline{U}_{E_2}^{me_{E_2/k}}.$$

For each positive integers m and n, now we define a map $h^{m,n}$ by the composition

$$h^{m,n} : \overline{U}^m \overset{M}{\otimes} \overline{U}^n(k) \to \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \xrightarrow{h^2} H^2(k, \mu_p^{\otimes 2}).$$

Here, the latter h^2 is the Galois symbol on $\mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k)$ as in (3). We also denote by

$$\begin{aligned} h^{-1,-1} := h^2 :& \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \to H^2(k, \mu_p^{\otimes 2}) \\ h^{-1,m} :& \mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k) \to \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \xrightarrow{h^2} H^2(k, \mu_p^{\otimes 2}) \end{aligned}$$

by convention. Since the field k is a p-adic field, the target of $h^{m,n}$ is the Brauer group and is known to be $H^2(k, \mu_p^{\otimes 2}) \simeq \mathbb{Z}/p$. By calculating the kernel and the image of this map $h^{m,n}$ we determine the structure of the Mackey product of these Mackey functors $\overline{U}^m$ as follows.

Lemma 3.2. *Let k be a p-adic field which contains μ_p. Put $e_0 := e_0(k) := v_k(p)/(p-1)$. For any positive integer m and n, we have*
(i)

$$h^{-1,m} : \mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k) \xrightarrow{\simeq} \begin{cases} \mathbb{Z}/p, & \text{if } m \le pe_0, \\ 0, & \text{otherwise.} \end{cases}$$

(ii)

$$h^{0,m} : \overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k) \xrightarrow{\simeq} \begin{cases} \mathbb{Z}/p, & \text{if } m < pe_0, \\ 0, & \text{otherwise.} \end{cases}$$

(iii)

$$h^{m,n} : \overline{U}^m \overset{M}{\otimes} \overline{U}^n(k) \xrightarrow{\simeq} 0 \quad \text{if } m \ge pe_0.$$

The rest of this section is devoted to show this lemma. The proof is divided into the following two steps.

(a) First we calculate the image of $h^{m,n}$,
(b) Next we show the injectivity of these maps.

The assertion (a) is obtained from the calculation of the cup product. To show the assertion (b) here we basically follow Raskind and Spieß' proof of Lemma 4.2.1 in [8]; refinements of Tate's in [14], that is, the bijectivity of maps $h^{-1,-1}, h^{-1,0}, h^{0,0}$. Precisely, the proof is further divided into three steps:

(b1) For a symbol of the form $\{a,b\}_{k/k}$ in the Mackey product $\overline{U}^m \overset{M}{\otimes} \overline{U}^n(k)$, if $h^{m,n}(\{a,b\}_{k/k}) = 0$ then $\{a,b\}_{k/k} = 0$.
(b2) Let $S(k)$ be the subgroup of $\overline{U}^m \overset{M}{\otimes} \overline{U}^n(k)$ generated by the symbols $\{a,b\}_{k/k}$. Then $h^{m,n}$ is injective on $S(k)$.
(b3) $\overline{U}^m \overset{M}{\otimes} \overline{U}^n(k) = S(k)$.

The claims (b1) and (b3) are given by the same arguments as Raskind-Spieß. But we obtain (b2) by determining the structure of $S(k)$ directly.

(a) *Image of the maps $h^{m,n}$*. First we determine the image of the maps $h^{m,n}$. The Galois symbol map $h^{-1,-1} = h^2$ is composed from the cup product $\cup : H^1(k,\mu_p) \otimes H^1(k,\mu_p) \to H^2(k,\mu_p^{\otimes 2})$ on the Galois cohomology groups (2). It is characterized by the Hilbert symbol $(\ ,\ )_p : k^\times/p \otimes k^\times/p \to \mu_p$ as in the following commutative diagram (*cf.* [10], Chap. XIV):

$$\begin{array}{ccc} H^1(k,\mu_p) \otimes H^1(k,\mu_p) & \xrightarrow{\cup} & H^2(k,\mu_p^{\otimes 2}) \\ \simeq \uparrow & & \downarrow \simeq \\ k^\times/p \otimes k^\times/p & \xrightarrow{(\ ,\ )_p} & \mu_p \end{array} .$$

The orders of the image in $H^2(k,\mu_p^{\otimes 2}) \simeq \mu_p \simeq \mathbb{Z}/p$ by the Hilbert symbol are calculated as follows:

Lemma 3.3 ([3], Lem. 3.1)**.** *Let m and n be positive integers.*

(i)

$$\#(k^\times/p, \overline{U}_k^m)_p = \begin{cases} p, & \text{if } m \le pe_0, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If $p \nmid m$ or $p \nmid n$, then*

$$\#(\overline{U}_k^m, \overline{U}_k^n)_p = \begin{cases} p, & \textit{if } m+n \leq pe_0, \\ 0, & \textit{otherwise}. \end{cases}$$

(iii) *If $p \mid m$ and $p \mid n$, then*

$$\#(\overline{U}_k^m, \overline{U}_k^n)_p = \begin{cases} p, & \textit{if } m+n < pe_0, \\ 0, & \textit{otherwise}. \end{cases}$$

From the calculation above, the image of the product does not depend on an extension E/k, hence we obtain the images as required

$$\mathrm{Im}(h^{-1,m}) \simeq \begin{cases} \mathbb{Z}/p, & \text{if } m \leq pe_0, \\ 0, & \text{otherwise}. \end{cases}$$
$$\mathrm{Im}(h^{0,m}) \simeq \begin{cases} \mathbb{Z}/p, & \text{if } m < pe_0, \\ 0, & \text{otherwise}. \end{cases}$$
$$\mathrm{Im}(h^{m,n}) = 0, \quad \text{if } m \geq pe_0.$$

(b) *Injectivity of $h^{m,n}$.* We prepare the following lemmas corresponding to the claim (b1) above.

Lemma 3.4. *For any symbol of the form $\{a,b\}_{k/k}$ in $\overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k)$, if we assume $h^{0,m}(\{a,b\}_{k/k}) = 0$ then $\{a,b\}_{k/k} = 0$.*

Proof. For any symbol of the form $\{a,b\}_{k/k}$ in $\overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k)$ and assume that $h^{0,m}(\{a,b\}_{k/k}) = 0$. The symbol map is written by the Hilbert symbol $h^{0,m}(\{a,b\}_{k/k}) = (a,b)_p$ and thus a is in the image of the norm $N_{E/k} : \overline{U}_E^0 \to \overline{U}_k^0$ for $E = k(\sqrt[p]{b})$ ([2], Chap. IV, Prop. 5.1). Take $\widetilde{a} \in E^\times/p$ such that $N_{E/k}(\widetilde{a}) = a$. We obtain

$$\{a,b\}_{k/k} = \{N_{E/k}\widetilde{a}, b\}_{k/k} = \{\widetilde{a}, \mathrm{Res}_{E/k}(b)\}_{E/k} = 0$$

by the projection formula, that is the condition (PF) in the definition of the product of the Mackey functors (Def. 2.1). $\square$

Next we show the vanishing results in Lemma 3.2:

$$\mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k) = 0, \quad \text{for any } m > pe_0,$$
$$\overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k) = 0, \quad \text{for any } m \geq pe_0,$$
$$\overline{U}^m \overset{M}{\otimes} \overline{U}^n(k) = 0, \quad \text{for any } m \geq pe_0.$$

Proof. The first equality follows from $\overline{U}_k^m = 0$ for $m > pe_0$ (Lem. 3.1). The third one is obtained from the second. To show the second equality by the norm arguments, it is enough to show that $\{a, b\}_{k/k} = 0$. Because of $\overline{U}_k^m = 0$ for $m > pe_0$ again, only the case $m = pe_0$ remains to prove. For the symbol $\{a, b\}_{k/k}$, we have $h^{0,m}(\{a, b\}_{k/k}) = (a, b)_p = 0$ by Lemma 3.3 and Lemma 3.4 shows $\{a, b\}_{k/k} = 0$. □

Proof of Lem. 3.2 (i). For any positive integers $m \leq pe_0$, by the bijectivity of $h^{-1,-1} = h^2$ ([8], Lem. 4.2.1) and the calculation of the image of $h^{-1,m}$ above, we have the surjections

$$\mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^{pe_0}(k) \twoheadrightarrow \mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k) \twoheadrightarrow \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \xrightarrow{\simeq} \mathbb{Z}/p.$$

Thus we may assume $m = pe_0$. Consider the following short exact sequence:

$$\overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0} \to \mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^{pe_0} \to \mathcal{Z}/p \overset{M}{\otimes} \overline{U}^{pe_0} \to 0,$$

where $\mathcal{Z}/p := (\mathbb{G}_m/p)/\overline{U}^0$. The product $\overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0}(k)$ is trivial from the above. Define the subgroup $S(k)$ of $\mathcal{Z}/p \overset{M}{\otimes} \overline{U}^{pe_0}(k)$ generated by the symbols of the form $\{a, b\}_{k/k}$. From Lemma 3.1 and Lemma 3.3, we have

$$\mathbb{Z}/p \simeq (k^\times/p)/\overline{U}_k^0 \otimes_{\mathbb{Z}} \overline{U}_k^{pe_0} \twoheadrightarrow S(k) \overset{h}{\twoheadrightarrow} \mathbb{Z}/p.$$

Thus the Galois symbol h is bijective on $S(k)$.

Finally, we show that $S(k)$ generates $\mathcal{Z}/p \overset{M}{\otimes} \overline{U}^{pe_0}(k)$. To show this, take a symbol $\{a, b\}_{E/k} \neq 0$ for any finite extension E/k.

E/k is unramified: Assume that the extension E/k is unramified. Then the norm map $\mathrm{N}_{E/k} : \overline{U}_E^{pe_0} \to \overline{U}_k^{pe_0}$ is surjective ([10], Chap. V, Sect. 2). There exist $c \in \mathcal{Z}/p(k)$ and $\widetilde{d} \in \overline{U}_E^{pe_0}$ such that $\{c, N_{E/k}(\widetilde{d})\}_{k/k}$ is a generator of $S(k) \simeq \mathbb{Z}/p$. By the equality

$$\{c, N_{E/k}(\widetilde{d})\}_{k/k} = \{\mathrm{Res}_{E/k}(c), \widetilde{d}\}_{E/k} = N_{E/k}(\{\mathrm{Res}_{E/k}(c), \widetilde{d}\}_{E/E}),$$

the symbol $\{\mathrm{Res}_{E/k}(c), \widetilde{d}\}_{E/E}$ is also a generator of $S(E) \simeq \mathbb{Z}/p$. For some i we have $\{a,b\}_{E/E} = \{\mathrm{Res}_{E/k}(c), \widetilde{d}^i\}_{E/E}$ and hence

$$\begin{aligned}
\{a,b\}_{E/k} &= N_{E/k}(\{a,b\}_{E/E}) \\
&= N_{E/k}(\{\mathrm{Res}_{E/k}(c), \widetilde{d}^i\}_{E/E}) \\
&= \{\mathrm{Res}_{E/k}(c), \widetilde{d}^i\}_{E/k} \\
&= \{c, N_{E/k}(\widetilde{d}^i)\}_{k/k}.
\end{aligned}$$

Therefore $\{a,b\}_{E/k} \in S(k)$.

E/k is totally ramified: Assume that E/k is totally ramified. In this case, the induced norm map on $\mathcal{Z}/p(E) \to \mathcal{Z}/p(k)$ is an isomorphism. There exist $\widetilde{c} \in \mathcal{Z}/p(E)$ and $d \in \overline{U}_k^{pe_0}$ such that $\{N_{E/k}(\widetilde{c}), d)\}_{k/k}$ is a generator of $S(k)$. Similar to the above proof, for some i we have

$$\begin{aligned}
\{a,b\}_{E/k} &= N_{E/k}(\{\widetilde{c}^i, \mathrm{Res}_{E/k}(d)\}_{E/E}) \\
&= \{N_{E/k}(\widetilde{c}^i), d\}_{k/k}.
\end{aligned}$$

E/k is an arbitrary extension: Take the maximal unramified subextension $k' \subset E$ over k. The assertion follows from

$$\{a,b\}_{E/k} = N_{E/k}(\{a,b\}_{E/E}) = N_{k'/k} \circ N_{E/k'}(\{a,b\}_{E/E}).$$

Therefore $\{a,b\}_{E/k} \in S(k)$ and thus $\mathbb{Z}/p \simeq S(k) = \mathcal{Z}/p \otimes \overline{U}^{pe_0}(k)$. □

Finally we show the rest of the assertions, namely the injectivity (and hence bijectivity) of

$$h^{0,m} : \overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k) \to H^2(k, \mu_p^{\otimes 2}) \simeq \mathbb{Z}/p$$

for any $m < pe_0$.

Proof of Lem. 3.2 (ii). Since we have surjections

$$\overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0-1}(k) \twoheadrightarrow \overline{U}^0 \overset{M}{\otimes} \overline{U}^m(k) \twoheadrightarrow \overline{U}^0 \overset{M}{\otimes} \overline{U}^0(k) \xrightarrow{\simeq} \mathbb{Z}/p,$$

we may assume that $m = pe_0 - 1$. We denote by $S(k)$ the subgroup of $\overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0-1}(k)$ generated by the symbols of the form $\{a,b\}_{k/k}$ $(a \in \overline{U}_k^0 = \overline{U}_k^1, b \in$

$\overline{U}_k^{pe_0-1}$). By Lemma 3.4 if a symbol of the form $\{a,b\}_{k/k}$ in $\overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0-1}(k)$ satisfies $h(\{a,b\}_{k/k}) = 0$ then $\{a,b\}_{k/k} = 0$, where $h = h^{0,pe_0-1} : \overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0-1}(k) \twoheadrightarrow H^2(k, \mu_p^{\otimes 2}) \simeq \mathbb{Z}/p$. Thus the natural surjection $\overline{U}_k^1 \otimes \overline{U}_k^{pe_0-1} \twoheadrightarrow S(k)$ factors through $\overline{U}_k^1/\overline{U}_k^2 \otimes \overline{U}_k^{pe_0-1}/\overline{U}_k^{pe_0}$ by Lemma 3.3. Fix a uniformizer π of k and consider the map

$$\mathbb{F} \longrightarrow \overline{U}_k^1/\overline{U}_k^2 \otimes \overline{U}_k^{pe_0-1}/\overline{U}_k^{pe_0}$$

defined by $x \mapsto (1 + \widetilde{x}^{-1}\pi) \otimes (1 + \pi^{pe_0-1})$, where $\widetilde{x} \in \mathcal{O}_k^\times$ is a lift of x. We denote by ϕ the composite

$$\phi : \mathbb{F} \to \overline{U}_k^1/\overline{U}_k^2 \otimes \overline{U}_k^{pe_0-1}/\overline{U}_k^{pe_0} \twoheadrightarrow S(k).$$

By the calculation of symbols (*cf.* [1], Lem. 4.1), we have

$$\begin{aligned} h(\phi(x)) &= (1 + \widetilde{x}^{-1}\pi, 1 + \pi^{pe_0-1})_p \\ &= (1 + \widetilde{x}^{-1}\pi, 1 + (1\widetilde{x}^{-1}\pi)\pi^{pe_0-1})_p \\ &= (1 + \widetilde{x}\pi^{pe_0}, \pi)_p. \end{aligned}$$

Define the group homomorphism $\sigma : \mathbb{F} \to \mathbb{F}$ by $x \mapsto x^p + ax$, where a is the class in $\mathbb{F}$ represented by $p\pi^{-e}$. By the equality (*cf.* [1], Lem. 5.1)

$$\begin{aligned} h(\phi(x^p + ax)) &= (1 + \widetilde{x}^p + p\pi^{-e}\widetilde{x}, \pi)_p \\ &= ((1 + \widetilde{x}\pi^{e_0})^p, \pi)_p \\ &= 0, \end{aligned}$$

and Lemma 3.4, the map ϕ factors through $\mathbb{F}/\sigma(\mathbb{F})$. On the other hand, the map σ is extended to $\sigma : \overline{\mathbb{F}} \to \overline{\mathbb{F}}$ and we have $H^1(\mathbb{F}, \overline{\mathbb{F}}) = 1$. Since $\mathrm{Ker}(\sigma) \simeq \mathbb{Z}/p$ as Galois modules, we obtain $\mathbb{F}/\sigma(\mathbb{F}) \simeq H^1(\mathbb{F}, \mathrm{Ker}(\sigma)) \simeq \mathbb{Z}/p$. Now we have the following commutative diagram

$$\begin{tikzcd} \mathbb{F}/\sigma(\mathbb{F}) \arrow[r, hook, "\phi"] \arrow[dr, "\simeq"'] & S(k) \arrow[d, "h"] \\ & \mathbb{Z}/p. \end{tikzcd}$$

For any symbol $\{a,b\}_{k/k}$ in $S(k)$, if we assume that the symbol $\{a,b\}_{k/k}$ is not contained in the image of ϕ, then we have $h(\{a,b\}_{k/k}) = 0$. But Lemma

3.4 implies $\{a,b\}_{k/k} = 0$ this contradicts to $\{a,b\}_{k/k} \notin \mathrm{Im}(\phi)$. Hence the map ϕ is bijective and we obtain $h : S(k) \xrightarrow{\simeq} \mathbb{Z}/p$.

Finally we show that $S(k) = \overline{U}^0 \overset{M}{\otimes} \overline{U}^{pe_0-1}(k)$ as the claim (b3). Take a symbol $\{a,b\}_{E/k} \neq 0$ and prove that it is in $S(k)$ by induction on the exponent of p in $e_{E/k}$. *The case* $p \nmid e_{E/k}$. In this extension E/k, the norm map $N_{E/k} : \overline{U}^0_E \to \overline{U}^0_k$ is surjective. There exist $\widetilde{c} \in U^0_E$ and $d \in U^{pe_0-1}_k$ such that $\{N_{E/k}(\widetilde{c}), d\}_{k/k}$ is a generator of $S(k) \simeq \mathbb{Z}/p$. By the projection formula, we have

$$\{N_{E/k}(\widetilde{c}), d\}_{k/k} = \{\widetilde{c}, \mathrm{Res}_{E/k}(d)\}_{E/k} = N_{E/k}(\{\widetilde{c}, \mathrm{Res}_{E/k}(d)\}_{E/E}).$$

Because of the symbol $\{\widetilde{c}, \mathrm{Res}_{E/k}(d)\}_{E/E}$ is also a generator of $S(E)$, for some i we obtain

$$\begin{aligned}\{a,b\}_{E/k} &= N_{E/k}(\{\widetilde{c}^i, \mathrm{Res}_{E/k}(d)\}_{E/E}) \\ &= \{N_{E/k}(\widetilde{c}^i), d\}_{k/k}.\end{aligned}$$

The case $p \mid e_{E/k}$. There exists a finite extension M/E of degree prime to p and an intermediate field M_1 of M/k such that M/M_1 is a cyclic and totally ramified extension of degree p. The norm map $N_{M/E} : U^0_M/p \to U^0_E/p$ is surjective and we have $\{a,b\}_{E/k} = \{N_{M/E}(\widetilde{a}), b\}_{E/k} = \{\widetilde{a}, \mathrm{Res}_{M/E}(b)\}_{M/k}$ for some $\widetilde{a} \in \overline{U}^0_M$. There exists an element $c \in \overline{U}^{(pe_0-1)e_{M_1/k}}_{M_1}$ such that $\Sigma = M_1(\sqrt[p]{c})$ is a totally ramified nontrivial extension of M_1 and $\Sigma \neq M$. In fact if the element c is in $\overline{U}^i_{M_1} \smallsetminus (\overline{U}^{i+1}_{M_1})$ ($(pe_0-1)e_{M_1/k} < i < pe_0(M_1) = pe_0 e_{M_1/k}, p \nmid i$) then the upper ramification subgroups of $G := \mathrm{Gal}(\Sigma/M_1)$ ([10], Chap. IV) is known to be

$$G = G^0 = G^1 = \cdots = G^{pe_0(M_1)-i} \supset G^{pe_0(M_1)-i+1} = 1$$

([4], Lem. 2.1.5, see also [10], Chap. V, Sect. 3). Hence we can choose c such that the ramification break of G is different from the one of $\mathrm{Gal}(M/M_1)$. Thus $N_{\Sigma/M_1}(U_\Sigma) + N_{M/M_1}(U_M) = U_{M_1}$ and we can take a symbol $\{N_{M/M_1}(\widetilde{d}), c\}_{M_1/M_1}$ such that it is a generator of $S(M_1)$ for some $\widetilde{d} \in \overline{U}^0_M$ and thus $\{\widetilde{d}, \mathrm{Res}_{M/M_1}(c)\}_{M/M}$

is also a generator of $S(M)$. Therefore, for some i, we have

$$\begin{aligned}
\{a,b\}_{E/k} &= \{\widetilde{a}, \mathrm{Res}_{M/E}(b)\}_{M/k} \\
&= N_{M/k}\{\widetilde{a}, \mathrm{Res}_{M/E}(b)\}_{M/M} \\
&= N_{M/k}\{\widetilde{d^i}, \mathrm{Res}_{M/M_1}(c)\}_{M/M} \\
&= N_{M_1/k} \circ N_{M/M_1}\{\widetilde{d^i}, \mathrm{Res}_{M/M_1}(c)\}_{M/M} \\
&= N_{M_1/k}\{\widetilde{d^i}, \mathrm{Res}_{M/M_1}(c)\}_{M/M_1} \\
&= N_{M_1/k}\{N_{M/M_1}(\widetilde{d^i}), c\}_{M_1/M_1} \\
&= \{N_{M/M_1}(\widetilde{d^i}), c\}_{M_1/k}.
\end{aligned}$$

From the induction hypothesis, the symbol $\{a,b\}_{E/k}$ is in $S(k)$. $\square$

4 Galois symbol for elliptic curves

We keep the notation as in the last section: k is a p-adic field assuming $p \neq 2$ with residue field $\mathbb{F} = \mathcal{O}_k/\mathfrak{m}_k$ and $e_0 = v_k(p)/(p-1)$. In this section, we study the Galois symbol map associated to elliptic curves over the p-adic field k.

The first main result here is the following theorem:

Theorem 4.1. *Let X be an elliptic curve over k with $X[p^n] \subset X(k)$. The Galois symbol map*

$$h^2_X : K(k; \mathbb{G}_m, X)/p^n \to H^2(k, \mathbb{G}_m[p^n] \otimes X[p^n])$$

is injective.

We use the results on the image of the symbol map in the case of $n = 1$ especially, that is the works after Berkovič and Kawachi ([4], see also [3], Thm. 3.3, Thm. 3.5).

For an elliptic curve X over k with $X[p] \subset X(k)$, fix an isomorphism of the Galois modules $X[p] \simeq (\mu_p)^{\oplus 2}$. From the isomorphism, we can identify $H^1(k, X[p])$ and $(k^\times/p)^{\oplus 2}$. On the latter group $k^\times/p$, the higher unit groups $U_k^m = 1 + \mathfrak{m}_k^m$ induce a filtration $\overline{U}_k^m := \mathrm{Im}(U_k^m \to k^\times/p)$ as noted in the last section. In terms of this filtration, the image of $h^1_X : X(k)/p \hookrightarrow$

$H^1(k, X[p]) = (k^\times/p)^{\oplus 2}$ is written precisely as follows (*cf.* [13]):

$$\mathrm{Im}(h^1_X) = \begin{cases} \overline{U}_k^0 \oplus \overline{U}_k^{pe_0} & \text{if } X\text{: ordinary,} \\ \overline{U}_k^{p(e_0-t_0)} \oplus \overline{U}_k^{pt_0} & \text{if } X\text{: super singular,} \\ k^\times/p \oplus 1 & \text{if } X\text{: split multiplicative.} \end{cases} \tag{4}$$

Here the invariant $t_0 := t_0(k)$ is defined by

$$t_0(k) = \max\{i \mid P \in \widehat{X}(\mathfrak{m}_k^i) \text{ for all } Q \in \widehat{X}[p]\} \tag{5}$$

where $\widehat{X}$ is the formal group associated to X. Note also the invariant t_0 satisfies $0 < t_0 < e_0$ and is calculated from the theory of the canonical subgroup of Katz-Lubin (*cf.* [3], Thm. 3.5).

By Lemma 2.4, Theorem 4.1 is reduced to showing the slightly stronger theorem below than the required.

Theorem 4.2. *Let X be an elliptic curve over k with $X[p] \subset X(k)$. The Galois symbol map on the Mackey product*

$$h^2_X : \mathbb{G}_m/p \overset{M}{\otimes} X/p(k) \to H^2(k, \mu_p \otimes X[p])$$

is injective.

Proof. Fix an isomorphism of the Galois modules $X[p] \simeq \mu_p^{\oplus 2}$ as above. For each point $P \in X(E)$ with image $\overline{P}$ in $X(E)/p$, we denote its image in $(E^\times/p)^{\oplus 2}$ by $h^1_X(\overline{P}) = (\overline{x}_P, \overline{y}_P)$. There exist points $P_x, P_y \in X(E)$ such that $h^1_X(\overline{P}_x) = (\overline{x}_P, 1)$ and $h^1_X(\overline{P}_y) = (1, \overline{y}_P)$. Thus we have $P \equiv P_x + P_y$ modulo p in $X(E)$. In the product $\mathbb{G}_m/p \overset{M}{\otimes} X/p(k)$ also, the following equality holds: For any $a \in E^\times$,

$$\{\overline{a}, \overline{P}\}_{E/k} = \{\overline{a}, \overline{P}_x\}_{E/k} + \{\overline{a}, \overline{P}_y\}_{E/k}$$

in $\mathbb{G}_m/p \overset{M}{\otimes} X/p(k)$. Let S_x be the subgroup of $\mathbb{G}_m/p \overset{M}{\otimes} X/p(k)$ generated by the symbols of the form $\{\overline{a}, \overline{P}_x\}_{E/k}$. Precisely, P_x is the point in $X(E)$ satisfying $\mathrm{pr}_y \circ h^1(\overline{P}_x) = 1 \in \overline{U}_E^{pt_0 e_{E/k}}$ where $\mathrm{pr}_y : (E^\times/p)^{\oplus 2} \to E^\times/p; (x,y) \mapsto y$ is the projection. Define S_y by the subgroup generated by the symbols $\{\overline{a}, \overline{P}_y\}_{E/k}$ similarly. Identifying $H^2(k, \mathbb{G}_m[p] \otimes X[p]) \simeq H^2(k, \mu_p^{\otimes 2})^{\oplus 2}$, the Galois symbol induces

$$h_x : S_x \hookrightarrow \mathbb{G}_m/p \overset{M}{\otimes} X/p(k) \xrightarrow{h} H^2(k, \mu_p^{\otimes 2})^{\oplus 2} \xrightarrow{pr_x} H^2(k, \mu_p^{\otimes 2}),$$

where pr_x is the first projection. Define $h_y : S_y \to H^2(k, \mu_p^{\otimes 2})$ in the same way. The description of the Galois symbol (2) indicates that for any symbol $\{\overline{a}, \overline{P}\}_{E/k}$, we have

$$h(\{\overline{a}, \overline{P}\}_{E/k}) = (h_x(\{\overline{a}, \overline{P}_x\}_{E/k}), h_y(\{\overline{a}, \overline{P}_y\}_{E/k}))$$

in $H^2(k, \mu_p^{\otimes 2})^{\oplus 2}$. Thus it is enough to show the injectivity of h_x and h_y.

Fix a primitive p-th roof of unity $\zeta \in \mu_p$. Let C be a subgroup of $X[p]$ generated by the point corresponding to $(\zeta, 1) \in \mu_p^{\oplus 2}$. The quotient $Y := X/C$ gives a commutative diagram:

$$\begin{tikzcd} X \arrow[rr, "p"] \arrow[dr, "\phi"'] & & X \\ & Y \arrow[ur, "\psi"'] & \end{tikzcd},$$

where ϕ and ψ are the induced isogenies. As in Section 2, we obtain the two Mackey functors $Y/\phi X$ and $X/\psi Y$ defined by the cokernels of ϕ and ψ respectively. By the very definition, ϕ is an isogeny of degree p with $X[\phi] = C \simeq \mu_p \oplus 1 \subset (\mu_p)^{\oplus 2}$. The inclusion $i : E^\times/p \to (E^\times/p)^{\oplus 2}; x \mapsto (x, 1)$ gives the commutative diagram

$$\begin{tikzcd} Y(E)/\phi X(E) \arrow[r, hook, "h^1_\phi"] \arrow[d, hook, "\psi"] & H^1(E, X[\phi]) \arrow[r, equal] \arrow[d, hook] & E^\times/p \arrow[d, hook, "i"] \\ X(E)/p \arrow[r, hook, "h^1"] & H^1(E, X[p]) \arrow[r, equal] & (E^\times/p)^{\oplus 2}. \end{tikzcd}$$

Thus the group $Y(E)/\phi X(E)$ is isomorphic to the group generated by the points of the form $\overline{P} = \overline{P}_x \in X(E)/p$ via ψ and we have the surjection $\mathbb{G}_m/p \overset{M}{\otimes} Y/\phi X(k) \to S_x$ defined by $\{a, Q\}_{E/k} \mapsto \{a, \psi(Q)\}_{E/k}$. This makes the following diagram commutative:

$$\begin{tikzcd} \mathbb{G}_m/p \overset{M}{\otimes} X/p(k) \arrow[r, "h^2_X"] & H^2(k, \mathbb{G}_m[p] \otimes X[p]) \\ S_x \arrow[u, hook] \arrow[r, "h_x"] & H^2(k, \mu_p^{\otimes 2}) \arrow[u, hook] \\ \mathbb{G}_m/p \overset{M}{\otimes} Y/\phi(k) \arrow[u, two heads] \arrow[r, "h_\phi"] & H^2(k, \mathbb{G}_m[p] \otimes X[\phi]), \arrow[u, "\simeq"'] \end{tikzcd}$$

We show that the lower map h_ϕ is injective under the assumptions $p \neq 2$ and $X[p] \subset X(k)$ (and thus $\mu_p \subset k$ by the Weil pairing). The elliptic curve X has at worst split multiplicative reduction, that means X has neither additive nor non-split multiplicative reduction over K ([4], Lem. 4.1.2). We show only the case the elliptic curve X has the supersingular good reduction. Other cases (X has split multiplicative reduction or ordinary reduction) can be proved similarly.

Let $\overline{U}^m$ be the Mackey functor defined by $E \mapsto \overline{U}_E^{me_{E/k}}$ as a subfunctor of $\mathbb{G}_m/p$. From (4), for any finite extension E/k, the image of the injection $h_X^1 : X(E)/p \hookrightarrow H^1(E, X[p]) = (E^\times/p)^{\oplus 2}$ is written as

$$\mathrm{Im}(h_X^1) = \overline{U}_E^{p(e_0(E)-t_0(E))} \oplus \overline{U}_E^{pt_0(E)}.$$

Here, $e_0(E) = e_0 e_{E/k}$ and $t_0(E) = t_0 e_{E/k}$ where $e_{E/k}$ is the ramification index of the extension E/k. For each m, the map $h^{-1,m}$ on $\mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k)$ (**??**) is the composition

$$h^{-1,m} : \mathbb{G}_m/p \overset{M}{\otimes} \overline{U}^m(k) \to \mathbb{G}_m/p \overset{M}{\otimes} \mathbb{G}_m/p(k) \xrightarrow{h^2} H^2(k, \mu_p^{\otimes 2}). \tag{6}$$

We identify the Mackey functor Y/ϕ with $\overline{U}^{p(e_0-t_0)}$ and the injectivity of h_ϕ follows from Lemma 3.2 (i). By identifying $X/\psi \simeq \overline{U}^{pt_0}$, the injectivity on S_y and thus Theorem 4.2 are also obtained Lemma 3.2 (i). □

Next, we study the Galois symbol map

$$h_{X,X'}^2 : K(k; X, X')/p^n \to H^2(k, X[p^n] \otimes X'[p^n])$$

associated to elliptic curves X and X' over k. The main result here is the following theorem:

Theorem 4.3. *Assume that $X[p^n] \subset X(k)$ and $X'[p^n] \subset X'(k)$ and X has split semi-ordinary reduction. Then, the Galois symbol map $h_{X,X'}^2$ is injective.*

Proof. From the induction on n and Lem. 2.4, it is enough to show the case of $n = 1$: the injectivity of

$$h_{X,X'}^2 : K(k; X, X')/p \to H^2(k, X[p] \otimes X'[p]).$$

Fix isomorphisms of the Galois modules $X[p] \simeq \mu_p^{\oplus 2}$ and $X'[p] \simeq \mu_p^{\oplus 2}$. As in the proof of Theorem 4.2, we identify the point $\overline{P} \in X(E)/p$ with $(\overline{x}_P, \overline{y}_P) \in$

$(E^\times/p)^{\oplus 2}$ in the image of the Kummer map h^1_X. There exist $\overline{P}_x$ and $\overline{P}_y$ corresponding to $(\overline{x}_P, 1)$ and $(1, \overline{y}_P)$ and we have $\overline{P} = \overline{P}_x + \overline{P}_y$. On the supersingular elliptic curve X' also the map h^1_X sends the point $\overline{P}' \in X'(E)/p$ to $(\overline{x}_P, \overline{y}_P) \in (E^\times/p)^{\oplus 2}$ we have $\overline{P}' = \overline{P}'_x + \overline{P}'_y$. Thus

$$\{\overline{P}, \overline{P}'\}_{E/k} = \{\overline{P}_x, \overline{P}'_x\}_{E/k} + \{\overline{P}_x, \overline{P}'_y\}_{E/k} + \{\overline{P}_y, \overline{P}'_x\} + \{\overline{P}_y, \overline{P}'_y\}_{E/k}$$

Let S_{xx}, S_{xy}, S_{yx} and S_{yy} be the subgroups of $X/p \overset{M}{\otimes} X'/p(k)$ generated by the symbols of the form $\{\overline{P}_x, \overline{P}'_x\}_{E/k}$, $\{\overline{P}_x, \overline{P}'_y\}_{E/k}$, $\{\overline{P}_y, \overline{P}'_x\}_{E/k}$, and $\{\overline{P}_y, \overline{P}'_y\}_{E/k}$ respectively, where E runs through all finite extension of k. Identifying $H^2(k, X[p] \otimes X'[p]) \simeq H^2(k, \mu_p^{\otimes 2})^{\oplus 4} \simeq \mathbb{Z}/p^{\oplus 4}$, the Galois symbol induces

$$h_{xx} : S_{xx} \hookrightarrow X/p \overset{M}{\otimes} X'/p(k) \overset{h_{X,X'}}{\to} H^2(k, \mu_p^{\otimes 2})^{\oplus 4} \overset{pr_{xx}}{\to} H^2(k, \mu_p^{\otimes 2}),$$

where pr_{xx} is the first projection. By the same way, we have $h_{xy} : S_{xy} \to H^2(k, \mu_p^{\otimes 2}), h_{yx} : S_{yx} \to H^2(k, \mu_p^{\otimes 2})$ and $h_{yy} : S_{yy} \to H^2(k, \mu_p^{\otimes 2})$ and it is enough to show the injectivity of these all maps.

Fix a primitive p-th root of unity $\zeta \in \mu_p$. Let C (resp. C') be a subgroup of $X[p]$ (resp. $X'[p]$) generated by the point corresponding to $(\zeta, 1) \in \mu_p^{\oplus 2}$. The quotients $Y := X/C$ and $Y' := X'/C'$ give p-isogenies $\phi : X \to Y, \psi : Y \to X$ and $\phi' : X' \to Y', \psi' : Y' \to X'$ as before. The isogenies ϕ and ϕ' induce the commutative diagram below

$$\begin{tikzcd}
S_{xx} \arrow[r, "h_{xx}"] & H^2(k, \mu_p^{\otimes 2}) \\
Y/\phi X \overset{M}{\otimes} Y'/\phi' X'(k) \arrow[u, two heads] \arrow[r, "h_{\phi,\phi'}"] & H^2(k, X[\phi] \otimes X'[\phi']). \arrow[u, "\simeq"']
\end{tikzcd}$$

By the same arguments on S_{xy}, S_{yx} and S_{yy}. The assertion is reduced to showing the injectivity of the maps $h_{\phi,\phi'}$, $h_{\phi,\psi'}$, $h_{\psi,\phi'}$ and $h_{\psi,\psi'}$.

(a) *X has split multiplicative reduction*: Consider the case that X has split multiplicative reduction. We also assume that X' has supersingular good reduction. Other cases on X' are treated in the same way and much easier. From (4), for any finite extension E/k, the images of the injections $h^1_X : X(E)/p \hookrightarrow H^1(E, X[p]) = (E^\times/p)^{\oplus 2}$ and $h^1_{X'} : X'(E)/p \hookrightarrow H^1(E, X'[p]) = (E^\times/p)^{\oplus 2}$ are written as

$$\mathrm{Im}(h^1_X) = E^\times/p \oplus 1,$$
$$\mathrm{Im}(h^1_{X'}) = \overline{U}_E^{p(e_0(E) - t'_0(E))} \oplus \overline{U}_E^{pt_0(E)}.$$

Here, $t_0'(E) = t_0' e_{E/k}$ is the invariant on X' defined by the same way as in (5). Therefore

$$Y/\phi \simeq \mathbb{G}_m/p, \quad X/\psi \simeq 1, \text{ and}$$
$$Y'/\phi' \simeq \overline{U}^{p(e_0 - t_0')}, \quad X'/\psi' \simeq \overline{U}^{pt_0'}.$$

Immediately, $X/\psi \overset{M}{\otimes} Y'/\phi'(k)$ and $X/\psi \overset{M}{\otimes} X'/\psi'(k)$ are trivial and thus $h_{\psi,\phi'}, h_{\psi,\psi'}$ are injective. The injectivity of $h_{\phi,\phi'}$ and $h_{\phi,\psi'}$ follow from Lemma 3.2 (i).

(b) *X has ordinary good reduction*: Next we assume that X has ordinary good reduction and X' is an supersingular elliptic curve over k. In this case, by (4) we have

$$Y/\phi \simeq \overline{U}^0, \quad X/\psi \simeq \overline{U}^{pe_0}, \text{ and}$$
$$Y'/\phi' \simeq \overline{U}^{p(e_0 - t_0')}, \quad X'/\psi' \simeq \overline{U}^{pt_0'}.$$

Identifying the above isomorphisms we have to show that the induced Galois symbol maps **??** on

$$\overline{U}^0 \overset{M}{\otimes} \overline{U}^{p(e_0 - t_0')}, \overline{U}^0 \overset{M}{\otimes} \overline{U}^{pt_0'}, \overline{U}^{pe_0} \overset{M}{\otimes} \overline{U}^{p(e_0 - t_0')}, \text{ and } \overline{U}^{pe_0} \overset{M}{\otimes} \overline{U}^{p(e_0 - t_0')}$$

are injective. However, the latter two are trivial by Lemma 3.2 (iii). The rest of the assertions follow from Lemma 3.2 (ii). □

5 Applications

Let X be an elliptic curves over a p-adic field k with $X[p^n] \subset X(k)$ and $k(X)$ the function field of X. For the multiplicative group $\mathbb{G}_m$ and the elliptic curve X, the Somekawa K-group has a description $K(k; \mathbb{G}_m, X) \xrightarrow{\simeq} V(X)$ ([11], Thm. 2.1), where $V(X)$ is the homology group of the complex

$$K_2(k(X)) \xrightarrow{\partial} \bigoplus_{P \in X:\ \text{closed points}} k(P)^{\times} \xrightarrow{N} k^{\times}$$

where $k(P)$ is the residue field at P, ∂ is defined by the tame symbols ∂_P as $\partial := \oplus_P \partial_P$ and N is the norm maps $N := \sum_P N_{k(P)/k}$. By the class field theory of curves over local field ([9], [18]), the group $V(X)$ has a relation

with the abelian fundamental group $\pi_1(X)^{\mathrm{ab}}$ as follows: The reciprocity map $\rho_X : SK_1(X) := \mathrm{Coker}(\partial) \to \pi_1(X)^{\mathrm{ab}}$ gives the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & V(X) \arrow[r] \arrow[d] & SK_1(X) \arrow[r] \arrow[d, "\rho_X"] & k^\times \arrow[d, "\rho_k"] & \\
0 \arrow[r] & \pi_1(X)^{\mathrm{ab,geo}} \arrow[r] & \pi_1(X)^{\mathrm{ab}} \arrow[r] & \mathrm{Gal}(k^{\mathrm{ab}}/k) \arrow[r] & 0,
\end{tikzcd}$$

where ρ_k denotes the reciprocity maps of local class field theory and $\pi_1(X)^{\mathrm{ab,geo}}$ is defined by the exactness. Furthermore, the geometric part of the fundamental group has the following structure

$$0 \to \pi_1(X)^{\mathrm{ab,geo}}_{\mathrm{tor}} \to \pi_1(X)^{\mathrm{ab,geo}} \to \widehat{\mathbb{Z}}^r \to 0,$$

where r is the dimension of the maximal split subtorus of the special fiber of the Néron model of X, and $\pi_1(X)^{\mathrm{ab,geo}}_{\mathrm{tor}}$ is the torsion subgroup. In particular, $r = 0$ if X has good reduction. The main theorem of the class field theory implies that the reciprocity map ρ_X induces $V(X)/p^n \simeq \pi_1(X)^{\mathrm{ab,geo}}_{\mathrm{tor}}/p^n$. From Corollary 1.2 we obtain

Theorem 5.1. *Under the assumption $X[p^n] \subset X(k)$, we have*

$$\pi_1(X)^{\mathrm{ab,geo}}_{\mathrm{tor}}/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } X\text{: split multiplicative,} \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \text{if } X\text{: good reduction.} \end{cases}$$

In particular, $\pi_1(X)^{\mathrm{ab,geo}}/p^n \simeq (\mathbb{Z}/p^n)^{\oplus 2}$ if X has good reduction.

Next we consider the the structure of the Chow group $\mathrm{CH}_0(X \times X')$ of 0-cycles on the product of elliptic curves X and X' over k. Let $A_0(X \times X)$ be the kernel of the degree map $\mathrm{CH}_0(X \times X') \to \mathbb{Z}$ and $T(X \times X')$ the kernel of the Albanese map $A_0(X \times X') \to X \times X'(k)$ for the abelian variety $X \times X'$, that is the so called Albanese kernel for $X \times X'$. These maps are surjective, and we have

$$\mathrm{CH}_0(X \times X')/T(X \times X') \simeq \mathbb{Z} \oplus (X \times X')(k).$$

If we assume p^n-torsion points $X[p^n]$ and $X'[p^n]$ are k-rational, Mattuck's theorem [5] implies $\mathrm{CH}_0(X \times X')/p^n \simeq (\mathbb{Z}/p^n)^{\oplus(2[k:\mathbb{Q}_p]+5)} \oplus T(X \times X')/p^n$ and the study of the structure of $\mathrm{CH}_0(X \times X')/p^n$ boils down to the calculation of

$T(X\times X')/p^n$. It is known that the Albanese kernel $T(X\times X')$ coincides with the Somekawa K-group $K(k;X,X')$ ([11], [8]). The cycle map ρ is compatible with the Galois symbol $h : K(k;X,X')/p^n \to H^2(k, X[p^n]\otimes X'[p^n])$ as in the following commutative diagram:

$$\begin{tikzcd} T(X\times X')/p^n \arrow[r, "\rho"] & H^4(X,\mathbb{Z}/p^n(2)) \\ K(k;X,X')/p^n \arrow[u, "\simeq"] \arrow[r, "h"] & H^2(k, X[p^n]\otimes X'[p^n]) \arrow[u, hook] \end{tikzcd}$$

Furthermore, the image of the cycle map $\rho : T(X\times X')/p^n \to H^4(X,\mathbb{Z}/p^n(2))$ is in $H^2(k, X[p^n]\otimes X'[p^n])$. We obtain the following:

Theorem 5.2. *Let X and X' be elliptic curves over k with good or split multiplicative reduction. Assume that X' is not a supersingular elliptic curve and $X[p^n]$ and $X'[p^n]$ are k-rational. Then, we have*

$$T(X\times X')/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } X \text{ and } X' \text{ have a same reduction type}, \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \text{if } X \text{ and } X' \text{ have different reduction types.} \end{cases}$$

References

[1] S. Bloch and K. Kato, *p-adic étale cohomology*, Inst. Hautes Études Sci. Publ. Math. (1986), 107–152.

[2] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002, With a foreword by I. R. Shafarevich.

[3] T. Hiranouchi and S. Hirayama, *On the cycle map for products of elliptic curves over a p-adic field*, preprint (2011).

[4] M. Kawachi, *Isogenies of degree p of elliptic curves over local fields and Kummer theory*, Tokyo J. Math. **25** (2002), 247–259.

[5] A. Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. (2) **62** (1955), 92–119.

[6] A. S. Merkur′ev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136.

[7] J. Murre and D. Ramakrishnan, *Local Galois symbols on $E \times E$*, Motives and algebraic cycles, Fields Inst. Commun., vol. 56, Amer. Math. Soc., Providence, RI, 2009, pp. 257–291.

[8] W. Raskind and M. Spiess, *Milnor K-groups and zero-cycles on products of curves over p-adic fields*, Compositio Math. **121** (2000), 1–33.

[9] S. Saito, *Class field theory for curves over local fields*, J. Number Theory **21** (1985), no. 1, 44–80.

[10] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[11] M. Somekawa, *On Milnor K-groups attached to semi-abelian varieties*, K-Theory **4** (1990), no. 2, 105–119.

[12] M. Spiess and T. Yamazaki, *A counterexample to generalizations of the Milnor-Bloch-Kato conjecture*, J. K-Theory **4** (2009), no. 1, 77–90.

[13] T. Takemoto, *Zero-cycles on products of elliptic curves over p-adic fields*, Acta Arith. **149** (2011), no. 3, 201–214.

[14] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.

[15] C. Weibel, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), 346–372.

[16] T. Yamazaki, *On Chow and Brauer groups of a product of Mumford curves*, Math. Ann. **333** (2005), 549–567.

[17] ______, *Milnor K-group attached to a torus and Birch-Tate conjecture*, Internat. J. Math. **20** (2009), no. 7, 841–857.

[18] T. Yoshida, *Finiteness theorems in the class field theory of varieties over local fields*, J. Number Theory **101** (2003), no. 1, 138–150.

Toshiro Hiranouchi
Department of Mathematics, Graduate School of Science, Hiroshima University
1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 Japan
Email address: `hira@hiroshima-u.ac.jp`